SEMINARIO

Máster en Nuevas Tecnologías Electrónicas y Fotónicas

Facultad de Ciencias Físicas. UCM

Conferenciante:

Verónica Fernández Mármol

Instituto de Tecnologías Físicas y de la Información (ITEFI-CSIC)

Título:

¿Podemos proteger nuestra información ante el todopoderoso ordenador cuántico?

Aula: 8B

Día: 20 de enero de 2014

Hora: 9:30

Resumen:

Los numerosos avances en Computación y Criptografía Cuántica en las últimas décadas han dado pie al surgimiento de un nuevo paradigma en las Tecnologías de la Información basado en las leyes de la Mecánica Cuántica. Propiedades como la superposición y el entrelazado cuánticos hacen posible una nueva forma de computación con una capacidad de procesado exponencialmente superior a la computación clásica. En numerosos campos como la Medicina, Biología, Optoelectrónica etc., las tecnologías de la Información Cuántica permitirán desarrollar los modelos necesarios que faciliten la comprensión de multitud de fenómenos aún desconocidos y que posibilitaran el desarrollo de enormes avances en dichos campos. Sin embargo, en el campo de la Seguridad de la Información y de la Criptografía, la computación cuántica supone una seria amenaza, ya que pone en jaque la seguridad de la distribución de claves criptográficas en general y del comercio electrónico en particular. La única alternativa hasta la fecha para solucionar este problema lo constituye la Criptografía Cuántica, una forma de proteger la información que no se basa en funciones matemáticas como la criptografía actual sino en las mismas leyes cuánticas que controlan el mundo subatómico. El Principio de Incertidumbre de Heisenberg nos sirve de aliado y nos permite distribuir claves entre usuarios por primera vez en la historia con seguridad absoluta, ya que la presencia de un adversario en el canal es detectada.